Cisco

Exam Questions 300-710

Securing Networks with Cisco Firepower (SNCF)

NEW QUESTION 1
- (Exam Topic 5)
An organization wants to secure traffic from their branch office to the headquarter building using Cisco Firepower devices, They want to ensure that their Cisco Firepower devices are not wasting resources on inspecting the VPN traffic. What must be done to meet these requirements?

A. Configure the Cisco Firepower devices to ignore the VPN traffic using prefilter policies
B. Enable a flexconfig policy to re-classify VPN traffic so that it no longer appears as interesting traffic
C. Configure the Cisco Firepower devices to bypass the access control policies for VPN traffic.
D. Tune the intrusion policies in order to allow the VPN traffic through without inspection

Answer: C

Explanation:
When you configure the Cisco Firepower devices to bypass the access control policies for VPN traffic, the devices will not inspect the VPN traffic and thus will not waste resources on it. This is the best option to ensure that the VPN traffic is not wasting resources on the Cisco Firepower devices.
Reference:
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/219759-configure-bypass-policies-on-the

NEW QUESTION 2
- (Exam Topic 5)
An engineer is creating an URL object on Cisco FMC How must it be configured so that the object will match for HTTPS traffic in an access control policy?

A. Specify the protocol to match (HTTP or HTTPS).
B. Use the FQDN including the subdomain for the website
C. Define the path to the individual webpage that uses HTTPS.
D. Use the subject common name from the website certificate

Answer: B

NEW QUESTION 3
- (Exam Topic 5)
Which Cisco FMC report gives the analyst information about the ports and protocols that are related to the configured sensitive network for analysis?

A. Malware Report
B. Host Report
C. Firepower Report
D. Network Report

Answer: D

NEW QUESTION 4
- (Exam Topic 5)
A Cisco FTD device is running in transparent firewall mode with a VTEP bridge group member ingress interface What must be considered by an engineer tasked with specifying a destination MAC address for a packet trace?

A. The destination MAC address is optional if a VLAN ID value is entered
B. Only the UDP packet type is supported
C. The output format option for the packet logs unavailable
D. The VLAN ID and destination MAC address are optional

Answer: A

NEW QUESTION 5
- (Exam Topic 5)
A network administrator is configuring Snort inspection policies and is seeing failed deployment messages in Cisco FMC. What information should the administrator generate for Cisco TAC to help troubleshoot?

A. A "show tech" file for the device in question.
B. A "troubleshoot" file for the device in question.
C. A "troubleshoot" file for the Cisco FMC.
D. A "show tech" for the Cisco FMC.

Answer: B

NEW QUESTION 6
- (Exam Topic 5)
An engineer is configuring a second Cisco FMC as a standby device but is unable to register with the active unit. What is causing this issue?

A. The primary FMC currently has devices connected to it.
B. The code versions running on the Cisco FMC devices are different
C. The licensing purchased does not include high availability
D. There is only 10 Mbps of bandwidth between the two devices.

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firep

NEW QUESTION 7
- (Exam Topic 5)
Which feature is supported by IRB on Cisco FTD devices?

A. redundant interface
B. dynamic routing protocol
C. EtherChannel interface
D. high-availability cluster

Answer: B

NEW QUESTION 8
- (Exam Topic 5)
A network administrator wants to block traffic to a known malware site at https://www.badsite.com and all subdomains while ensuring no packets from any internal client are sent to that site. Which type of policy must the network administrator use to accomplish this goal?

A. Prefilter policy
B. SSL policy
C. DNS policy
D. Access Control policy with URL filtering

Answer: D

NEW QUESTION 9
- (Exam Topic 5)
A network engineer wants to add a third-party threat feed into the Cisco FMC for enhanced threat detection Which action should be taken to accomplish this goal?

A. Enable Threat Intelligence Director using STIX and TAXII
B. Enable Rapid Threat Containment using REST APIs
C. Enable Threat Intelligence Director using REST APIs
D. Enable Rapid Threat Containment using STIX and TAXII

Answer: A

NEW QUESTION 10
- (Exam Topic 5)
A network engineer is tasked with minimising traffic interruption during peak traffic limes. When the SNORT inspection engine is overwhelmed, what must be configured to alleviate this issue?

A. Enable IPS inline link state propagation
B. Enable Pre-filter policies before the SNORT engine failure.
C. Set a Trust ALL access control policy.
D. Enable Automatic Application Bypass.

Answer: D

NEW QUESTION 10
- (Exam Topic 5)
A network administrator configured a NAT policy that translates a public IP address to an internal web server IP address. An access policy has also been created that allows any source to reach the public IP address on port 80. The web server is still not reachable from the Internet on port 80. Which configuration change is needed?

A. The intrusion policy must be disabled for port 80.
B. The access policy rule must be configured for the action trust.
C. The NAT policy must be modified to translate the source IP address as well as destination IP address.
D. The access policy must allow traffic to the internal web server IP address.

Answer: D

NEW QUESTION 14
- (Exam Topic 5)
A security engineer is adding three Cisco FTD devices to a Cisco FMC. Two of the devices have successfully registered to the Cisco FMC. The device that is unable to register is located behind a router that translates all outbound traffic to the router's WAN IP address. Which two steps are required for this device to register to the Cisco FMC? (Choose two.)

A. Reconfigure the Cisco FMC lo use the device's private IP address instead of the WAN address.
B. Configure a NAT ID on both the Cisco FMC and the device.
C. Add the port number being used for PAT on the router to the device's IP address in the Cisco FMC.
D. Reconfigure the Cisco FMC to use the device's hostname instead of IP address.
E. Remove the IP address defined for the device in the Cisco FMC.

Answer: BE

NEW QUESTION 17

- (Exam Topic 5)
An organization is implementing Cisco FTD using transparent mode in the network. Which rule in the default Access Control Policy ensures that this deployment does not create a loop in the network?

A. ARP inspection is enabled by default.
B. Multicast and broadcast packets are denied by default.
C. STP BPDU packets are allowed by default.
D. ARP packets are allowed by default.

Answer: B

NEW QUESTION 19
- (Exam Topic 5)
What is the advantage of having Cisco Firepower devices send events to Cisco Threat Response via the security services exchange portal directly as opposed to using syslog?

A. All types of Cisco Firepower devices are supported.
B. An on-premises proxy server does not need to be set up and maintained.
C. Cisco Firepower devices do not need to be connected to the Internet.
D. Supports all devices that are running supported versions of Cisco Firepower.

Answer: B

NEW QUESTION 22
- (Exam Topic 5)
A security engineer needs to configure a network discovery policy on a Cisco FMC appliance and prevent excessive network discovery events from overloading the FMC database? Which action must be taken to accomplish this task?

A. Change the network discovery method to TCP/SYN.
B. Configure NetFlow exporters for monitored networks.
C. Monitor only the default IPv4 and IPv6 network ranges.
D. Exclude load balancers and NAT devices in the policy.

Answer: D

NEW QUESTION 26
- (Exam Topic 5)
An engineer defines a new rule while configuring an Access Control Policy. After deploying the policy, the rule is not working as expected and the hit counters associated with the rule are showing zero. What is causing this error?

A. Logging is not enabled for the rule.
B. The rule was not enabled after being created.
C. The wrong source interface for Snort was selected in the rule.
D. An incorrect application signature was used in the rule.

Answer: B

NEW QUESTION 28
- (Exam Topic 5)
An engineer is investigating connectivity problems on Cisco Firepower that is using service group tags.
Specific devices are not being tagged correctly, which is preventing clients from using the proper policies when going through the firewall How is this issue resolved?

A. Use traceroute with advanced options.
B. Use Wireshark with an IP subnet filter.
C. Use a packet capture with match criteria.
D. Use a packet sniffer with correct filtering

Answer: C

NEW QUESTION 29
- (Exam Topic 5)
The network administrator wants to enhance the network security posture by enabling machine learning tor malware detection due to a concern with suspicious Microsoft executable file types that were seen while creating monthly security reports for the CIO. Which feature must be enabled to accomplish this goal?

A. Spero
B. dynamic analysis
C. static analysis
D. Ethos

Answer: A

NEW QUESTION 33
- (Exam Topic 5)
An engineer wants to add an additional Cisco FTD Version 6.2.3 device to their current 6.2.3 deployment to create a high availability pair.
The currently deployed Cisco FTD device is using local management and identical hardware including the available port density to enable the failover and stateful links required in a proper high availability deployment. Which action ensures that the environment is ready to pair the new Cisco FTD with the old one?

A. Change from Cisco FDM management to Cisco FMC management on both devices and register them to FMC.
B. Ensure that the two devices are assigned IP addresses from the 169 254.0.0/16 range for failover interfaces.
C. Factory reset the current Cisco FTD so that it can synchronize configurations with the new Cisco FTD device.
D. Ensure that the configured DNS servers match on the two devices for name resolution.

Answer: A

NEW QUESTION 35
- (Exam Topic 5)
An engineer is configuring multiple Cisco FTD appliances (or use in the network. Which rule must the engineer follow while defining interface objects in Cisco FMC for use with interfaces across multiple devices?

A. An interface cannot belong to a security zone and an interface group
B. Interface groups can contain multiple interface types
C. Interface groups can contain interfaces from many devices.
D. Two security zones can contain the same interface

Answer: C

NEW QUESTION 36
- (Exam Topic 5)
A network administrator notices that inspection has been interrupted on all non-managed interfaces of a device. What is the cause of this?

A. The value of the highest MTU assigned to any non-management interface was changed.
B. The value of the highest MSS assigned to any non-management interface was changed.
C. A passive interface was associated with a security zone.
D. Multiple inline interface pairs were added to the same inline interface.

Answer: A

NEW QUESTION 39
- (Exam Topic 5)
An administrator receives reports that users cannot access a cloud-hosted web server. The access control policy was recently updated with several new policy additions and URL filtering. What must be done to troubleshoot the issue and restore access without sacrificing the organization's security posture?

A. Create a new access control policy rule to allow ports 80 and 443 to the FQDN of the web server.
B. Identify the blocked traffic in the Cisco FMC connection events to validate the block, and modify the policy to allow the traffic to the web server.
C. Verify the blocks using the packet capture tool and create a rule with the action monitor for the traffic.
D. Download a PCAP of the traffic attempts to verify the blocks and use the flexconfig objects to create a rule that allows only the required traffic to the destination server.

Answer: B

NEW QUESTION 44
- (Exam Topic 5)
A network administrator is configuring a Cisco AMP public cloud instance and wants to capture infections and polymorphic variants of a threat to help detect families of malware. Which detection engine meets this requirement?

A. RBAC
B. Tetra
C. Ethos
D. Spero

Answer: C

NEW QUESTION 49
- (Exam Topic 5)
When using Cisco Threat Response, which phase of the Intelligence Cycle publishes the results of the investigation?

A. direction
B. dissemination
C. processing
D. analysis

Answer: B

Explanation:
Disseminate: The dissemination phase
publishes the results of the investigation or threat hunt. This
information is disseminated with a focus on the receivers of the information. At the tactical level, this information feeds back into the beginning of the F3EAD model, Find. Figure 3 illustrates the F3EAD model.

NEW QUESTION 52
- (Exam Topic 5)
A network administrator needs to create a policy on Cisco Firepower to fast-path traffic to avoid Layer 7 inspection. The rate at which traffic is inspected must be optimized. What must be done to achieve this goal?

A. Enable lhe FXOS for multi-instance.
B. Configure a prefilter policy.
C. Configure modular policy framework.
D. Disable TCP inspection.

Answer: B

NEW QUESTION 53
- (Exam Topic 5)
A network administrator is configuring an FTD in transparent mode. A bridge group is set up and an access policy has been set up to allow all IP traffic. Traffic is not passing through the FTD. What additional configuration is needed?

A. The security levels of the interfaces must be set.
B. A default route must be added to the FTD.
C. An IP address must be assigned to the BVI.
D. A mac-access control list must be added to allow all MAC addresses.

Answer: C

NEW QUESTION 58
- (Exam Topic 5)
With a recent summer time change, system logs are showing activity that occurred to be an hour behind real time Which action should be taken to resolve this issue?

A. Manually adjust the time to the correct hour on all managed devices
B. Configure the system clock settings to use NTP with Daylight Savings checked
C. Manually adjust the time to the correct hour on the Cisco FMC.
D. Configure the system clock settings to use NTP

Answer: B

NEW QUESTION 60
- (Exam Topic 5)
An engineer has been tasked with using Cisco FMC to determine if files being sent through the network are malware. Which two configuration tasks must be performed to achieve this file lookup? (Choose two).

A. The Cisco FMC needs to include a SSL decryption policy.
B. The Cisco FMC needs to connect to the Cisco AMP for Endpoints service.
C. The Cisco FMC needs to connect to the Cisco ThreatGrid service directly for sandboxing.
D. The Cisco FMC needs to connect with the FireAMP Cloud.
E. The Cisco FMC needs to include a file inspection policy for malware lookup.

Answer: BE

NEW QUESTION 62
- (Exam Topic 5)
IT management is asking the network engineer to provide high-level summary statistics of the Cisco FTD appliance in the network. The business is approaching a peak season so the need to maintain business uptime is high. Which report type should be used to gather this information?

A. Malware Report
B. Standard Report
C. SNMP Report
D. Risk Report

Answer: B

NEW QUESTION 66
- (Exam Topic 5)
An engineer is setting up a new Firepower deployment and is looking at the default FMC policies to start the implementation During the initial trial phase, the organization wants to test some common Snort rules while still allowing the majority of network traffic to pass Which default policy should be used?

A. Maximum Detection
B. Security Over Connectivity
C. Balanced Security and Connectivity
D. Connectivity Over Security

Answer: C

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-intrusio

NEW QUESTION 68
- (Exam Topic 5)
After using Firepower for some time and learning about how it interacts with the network, an administrator is trying to correlate malicious activity with a user Which widget should be configured to provide this visibility on the Cisco Firepower dashboards?

A. Custom Analysis

B. Current Status
C. Current Sessions
D. Correlation Events

Answer: A

NEW QUESTION 70
- (Exam Topic 5)
A network engineer is logged into the Cisco AMP for Endpoints console and sees a malicious verdict for an identified SHA-256 hash. Which configuration is needed to mitigate this threat?

A. Add the hash to the simple custom deletion list.
B. Use regular expressions to block the malicious file.
C. Enable a personal firewall in the infected endpoint.
D. Add the hash from the infected endpoint to the network block list.

Answer: A

NEW QUESTION 75
- (Exam Topic 5)
What is the role of the casebook feature in Cisco Threat Response?

A. sharing threat analysts
B. pulling data via the browser extension
C. triage automaton with alerting
D. alert prioritization

Answer: A

Explanation:
The casebook and pivot menu are widgets available in Cisco Threat Response. Casebook - It is used to record, organize, and share sets of observables of interest primarily during an investigation and threat analysis. You can use a casebook to get the current verdicts or dispositions on the observables.
https://www.cisco.com/c/en/us/td/docs/se curity/ces/user_guide/esa_user_guide_13-5-1/b_ESA_Admin_Guide_ces _13-5-1/b_ESA_Admin_Guide_13-0_chapter_0110001.pdf

NEW QUESTION 79
- (Exam Topic 5)
Which protocol is needed to exchange threat details in rapid threat containment on Cisco FMC?

A. SGT
B. SNMP v3
C. BFD
D. pxGrid

Answer: D

NEW QUESTION 83
- (Exam Topic 5)
An engineer is troubleshooting HTTP traffic to a web server using the packet capture tool on Cisco FMC. When reviewing the captures, the engineer notices that there are a lot of packets that are not sourced from or destined to the web server being captured. How can the engineer reduce the strain of capturing packets for irrelevant traffic on the Cisco FTD device?

A. Use the host filter in the packet capture to capture traffic to or from a specific host.
B. Redirect the packet capture output to a .pcap file that can be opened with Wireshark.
C. Use the -c option to restrict the packet capture to only the first 100 packets.
D. Use an access-list within the packet capture to permit only HTTP traffic to and from the web server.

Answer: A

NEW QUESTION 86
- (Exam Topic 5)
An engineer is troubleshooting connectivity to the DNS servers from hosts behind a new Cisco FTD device. The hosts cannot send DNS queries to servers in the DMZ. Which action should the engineer take to troubleshoot this issue using the real DNS packets?

A. Use the Connection Events dashboard to check the block reason and adjust the inspection policy as needed.
B. Use the packet capture tool to check where the traffic is being blocked and adjust the access control or intrusion policy as needed.
C. Use the packet tracer tool to determine at which hop the packet is being dropped.
D. Use the show blocks command in the Threat Defense CLI tool and create a policy to allow the blockedtraffic.

Answer: A

NEW QUESTION 88
- (Exam Topic 5)
A company wants a solution to aggregate the capacity of two Cisco FTD devices to make the best use of resources such as bandwidth and connections per second. Which order of steps must be taken across the Cisco FTDs with Cisco FMC to meet this requirement?

A. Configure the Cisco FTD interfaces, add members to FMC, configure cluster members in FMC, and create cluster in Cisco FMC.

B. Add members to Cisco FMC, configure Cisco FTD interfaces in Cisco FM
C. configure cluster members in Cisco FMC, create cluster in Cisco FM
D. and configure cluster members in Cisco FMC.
E. Configure the Cisco FTD interfaces and cluster members, add members to Cisco FM
F. and create the cluster in Cisco FMC.
G. Add members to the Cisco FMC, configure Cisco FTD interfaces, create the cluster in Cisco FMC, and configure cluster members in Cisco FMC.

Answer: D

NEW QUESTION 90
- (Exam Topic 5)
An engineer has been tasked with providing disaster recovery for an organization's primary Cisco FMC. What must be done on the primary and secondary Cisco FMCs to ensure that a copy of the original corporate policy is available if the primary Cisco FMC fails?

A. Configure high-availability in both the primary and secondary Cisco FMCs
B. Connect the primary and secondary Cisco FMC devices with Category 6 cables of not more than 10 meters in length.
C. Place the active Cisco FMC device on the same trusted management network as the standby device
D. Restore the primary Cisco FMC backup configuration to the secondary Cisco FMC device when the primary device fails

Answer: D

NEW QUESTION 91
- (Exam Topic 5)
An engineer is configuring a cisco FTD appliance in IPS-only mode and needs to utilize fail-to-wire interfaces. Which interface mode should be used to meet these requirements?

A. transparent
B. routed
C. passive
D. inline set

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/inline

NEW QUESTION 92
- (Exam Topic 5)
Which two routing options are valid with Cisco FTD? (Choose Two)

A. BGPv6
B. ECMP with up to three equal cost paths across multiple interfaces
C. ECMP with up to three equal cost paths across a single interface
D. BGPv4 in transparent firewall mode
E. BGPv4 with nonstop forwarding

Answer: AC

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config- guide-v601/fpmc-config-guide-v60_chapter_01100011.html#ID-2101-0000000e

NEW QUESTION 93
- (Exam Topic 5)
A network administrator is troubleshooting access to a website hosted behind a Cisco FTD device External clients cannot access the web server via HTTPS The IP address configured on the web server is 192 168 7.46 The administrator is running the command capture CAP interface outside match ip any 192.168.7.46 255.255.255.255 but cannot see any traffic in the capture Why is this occurring?

A. The capture must use the public IP address of the web server.
B. The FTD has no route to the web server.
C. The access policy is blocking the traffic.
D. The packet capture shows only blocked traffic

Answer: A

NEW QUESTION 97
- (Exam Topic 5)
A mid-sized company is experiencing higher network bandwidth utilization due to a recent acquisition The network operations team is asked to scale up their one Cisco FTD appliance deployment to higher capacities due to the increased network bandwidth. Which design option should be used to accomplish this goal?

A. Deploy multiple Cisco FTD appliances in firewall clustering mode to increase performance.
B. Deploy multiple Cisco FTD appliances using VPN load-balancing to scale performance.
C. Deploy multiple Cisco FTD HA pairs to increase performance
D. Deploy multiple Cisco FTD HA pairs in clustering mode to increase performance

Answer: A

NEW QUESTION 102
- (Exam Topic 5)
Upon detecting a flagrant threat on an endpoint, which two technologies instruct Cisco Identity Services Engine to contain the infected endpoint either manually or automatically? (Choose two.)

A. Cisco ASA 5500 Series
B. Cisco FMC
C. Cisco AMP
D. Cisco Stealthwatch
E. Cisco ASR 7200 Series

Answer: CD

NEW QUESTION 105
- (Exam Topic 4)
What is a valid Cisco AMP file disposition?

A. non-malicious
B. malware
C. known-good
D. pristine

Answer: B

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide- v60/Reference_a_wrapper_Chapter_topic_here.html

NEW QUESTION 110
- (Exam Topic 4)
Which action should you take when Cisco Threat Response notifies you that AMP has identified a file as malware?

A. Add the malicious file to the block list.
B. Send a snapshot to Cisco for technical support.
C. Forward the result of the investigation to an external threat-analysis engine.
D. Wait for Cisco Threat Response to automatically block the malware.

Answer: A

NEW QUESTION 113
- (Exam Topic 4)
Which connector is used to integrate Cisco ISE with Cisco FMC for Rapid Threat Containment?

A. pxGrid
B. FTD RTC
C. FMC RTC
D. ISEGrid

Answer: A

NEW QUESTION 117
- (Exam Topic 5)
An engineer must define a URL object on Cisco FMC. What is the correct method to specify the URL without performing SSL inspection?

A. Use Subject Common Name value.
B. Specify all subdomains in the object group.
C. Specify the protocol in the object.
D. Include all URLs from CRL Distribution Points.

Answer: B

NEW QUESTION 120
- (Exam Topic 3)
When do you need the file-size command option during troubleshooting with packet capture?

A. when capture packets are less than 16 MB
B. when capture packets are restricted from the secondary memory
C. when capture packets exceed 10 GB
D. when capture packets exceed 32 MB

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/troubleshooting_the_system.html

NEW QUESTION 123

- (Exam Topic 3)
What is the benefit of selecting the trace option for packet capture?

A. The option indicates whether the packet was dropped or successful.
B. The option indicated whether the destination host responds through a different path.
C. The option limits the number of packets that are captured.
D. The option captures details of each packet.

Answer: A

NEW QUESTION 127
- (Exam Topic 3)
What is a functionality of port objects in Cisco FMC?

A. to mix transport protocols when setting both source and destination port conditions in a rule
B. to represent protocols other than TCP, UDP, and ICMP
C. to represent all protocols in the same way
D. to add any protocol other than TCP or UDP for source port conditions in access control rules.

Answer: B

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/reusable_objects.html

NEW QUESTION 131
- (Exam Topic 4)
Which two features of Cisco AMP for Endpoints allow for an uploaded file to be blocked? (Choose two.)

A. application blocking
B. simple custom detection
C. file repository
D. exclusions
E. application whitelisting

Answer: AB

NEW QUESTION 134
- (Exam Topic 3)
Which limitation applies to Cisco Firepower Management Center dashboards in a multidomain environment?

A. Child domains can view but not edit dashboards that originate from an ancestor domain.
B. Child domains have access to only a limited set of widgets from ancestor domains.
C. Only the administrator of the top ancestor domain can view dashboards.
D. Child domains cannot view dashboards that originate from an ancestor domain.

Answer: D

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide- v60/Using_Dashboards.html

NEW QUESTION 135
- (Exam Topic 3)
Which group within Cisco does the Threat Response team use for threat analysis and research?

A. Cisco Deep Analytics
B. OpenDNS Group
C. Cisco Network Response
D. Cisco Talos

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/products/security/threat-response.html#~benefits

NEW QUESTION 136
- (Exam Topic 2)
Which two actions can be used in an access control policy rule? (Choose two.)

A. Block with Reset
B. Monitor
C. Analyze
D. Discover
E. Block ALL

Answer: AB

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa- firepower-module-user-guide-v541/AC-Rules-Tuning-Overview.html#71854

NEW QUESTION 138
- (Exam Topic 3)
Which two statements about deleting and re-adding a device to Cisco FMC are true? (Choose two.)

A. An option to re-apply NAT and VPN policies during registration is available, so users do not need to re- apply the policies after registration is completed.
B. Before re-adding the device in Cisco FMC, you must add the manager back in the device.
C. No option to delete and re-add a device is available in the Cisco FMC web interface.
D. The Cisco FMC web interface prompts users to re-apply access control policies.
E. No option to re-apply NAT and VPN policies during registration is available, so users need to re-apply the policies after registration is completed.

Answer: DE

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide- v60/Device_Management_Basics.html

NEW QUESTION 142
- (Exam Topic 3)
Which Cisco Firepower feature is used to reduce the number of events received in a period of time?

A. rate-limiting
B. suspending
C. correlation
D. thresholding

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa- firepower-module-user-guide-v541/Intrusion-Global-Threshold.html

NEW QUESTION 146
- (Exam Topic 3)
Which two packet captures does the FTD LINA engine support? (Choose two.)

A. Layer 7 network ID
B. source IP
C. application ID
D. dynamic firewall importing
E. protocol

Answer: BE

Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with- firepower-threat-defense-f.html

NEW QUESTION 149
- (Exam Topic 2)
In which two ways do access control policies operate on a Cisco Firepower system? (Choose two.)

A. Traffic inspection can be interrupted temporarily when configuration changes are deployed.
B. The system performs intrusion inspection followed by file inspection.
C. They can block traffic based on Security Intelligence data.
D. File policies use an associated variable set to perform intrusion prevention.
E. The system performs a preliminary inspection on trusted traffic to validate that it matches the trusted parameters.

Answer: AC

Explanation:
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Acces

NEW QUESTION 154
- (Exam Topic 2)
An administrator is creating interface objects to better segment their network but is having trouble adding interfaces to the objects. What is the reason for this failure?

A. The interfaces are being used for NAT for multiple networks.
B. The administrator is adding interfaces of multiple types.
C. The administrator is adding an interface that is in multiple zones.
D. The interfaces belong to multiple interface groups.

Answer: D

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusa "All interfaces in an interface object must be of the same type: all inline, passive, switched, routed, or ASA FirePOWER. After you create an interface object, you cannot change the type of interfaces it contains."

NEW QUESTION 159
- (Exam Topic 2)
What is the disadvantage of setting up a site-to-site VPN in a clustered-units environment?

A. VPN connections can be re-established only if the failed master unit recovers.
B. Smart License is required to maintain VPN connections simultaneously across all cluster units.
C. VPN connections must be re-established when a new master unit is elected.
D. Only established VPN connections are maintained when a new master unit is elected.

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster- solution.html#concept_g32_yml_y2b

NEW QUESTION 161
- (Exam Topic 2)
Which two OSPF routing features are configured in Cisco FMC and propagated to Cisco FTD? (Choose two.)

A. OSPFv2 with IPv6 capabilities
B. virtual links
C. SHA authentication to OSPF packets
D. area boundary router type 1 LSA filtering
E. MD5 authentication to OSPF packets

Answer: BE

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-v62/ospf_for_firepower_threat_defense.html

NEW QUESTION 162
- (Exam Topic 2)
Which Firepower feature allows users to configure bridges in routed mode and enables devices to perform Layer 2 switching between interfaces?

A. FlexConfig
B. BDI
C. SGT
D. IRB

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/relnotes/
Firepower_System_Release_Notes_Version_620/new_features_and_functionality.html

NEW QUESTION 165
- (Exam Topic 2)
Which command is run on an FTD unit to associate the unit to an FMC manager that is at IP address 10.0.0.10, and that has the registration key Cisco123?

A. configure manager local 10.0.0.10 Cisco123
B. configure manager add Cisco123 10.0.0.10
C. configure manager local Cisco123 10.0.0.10
D. configure manager add 10.0.0.10 Cisco123

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt- nw.html#id_106101

NEW QUESTION 167
- (Exam Topic 1)
An engineer must configure high availability for the Cisco Firepower devices. The current network topology does not allow for two devices to pass traffic concurrently. How must the devices be implemented in this environment?

A. in active/active mode
B. in a cluster span EtherChannel
C. in active/passive mode
D. in cluster interface mode

Answer: C

NEW QUESTION 170
- (Exam Topic 1)

Which Cisco Firepower Threat Defense, which two interface settings are required when configuring a routed interface? (Choose two.)

A. Redundant Interface
B. EtherChannel
C. Speed
D. Media Type
E. Duplex

Answer: CE

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/fdm/fptd-fdm-config-guide-610/fptd-fdm- interfaces.html

NEW QUESTION 175
- (Exam Topic 1)
Which interface type allows packets to be dropped?

A. passive
B. inline
C. ERSPAN
D. TAP

Answer: B

Explanation:
Reference:
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuring-firepower- threat-defense-int.html

NEW QUESTION 179
- (Exam Topic 1)
What is the difference between inline and inline tap on Cisco Firepower?

A. Inline tap mode can send a copy of the traffic to another device.
B. Inline tap mode does full packet capture.
C. Inline mode cannot do SSL decryption.
D. Inline mode can drop malicious traffic.

Answer: A

NEW QUESTION 182
- (Exam Topic 1)
Which protocol establishes network redundancy in a switched Firepower device deployment?

A. STP
B. HSRP
C. GLBP
D. VRRP

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config- guide-
v62/firepower_threat_defense_high_availability.html

NEW QUESTION 186
- (Exam Topic 1)
A network engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire How should this be implemented?

A. Specify the BVI IP address as the default gateway for connected devices.
B. Enable routing on the Cisco Firepower
C. Add an IP address to the physical Cisco Firepower interfaces.
D. Configure a bridge group in transparent mode.

Answer: D

Explanation:
Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place. Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the ASA uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.

NEW QUESTION 188
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

300-710 Practice Exam Features:

* 300-710 Questions and Answers Updated Frequently

* 300-710 Practice Questions Verified by Expert Senior Certified Staff

* 300-710 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 300-710 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 300-710 Practice Test Here